03 10-00

A

Assistant Commissioner for Patents
Washington, D.C. 20231
Sir:

ATTORNEY DOCKET NO. YOR000028US1 (8728-349)
Date: March 17, 2000
Express Mail Label: EL433927561US
Date of Deposit: March 17, 2000

Transmitted herewith for filing is the Patent Application of:

Inventors: Martin Kienzle, Ray E. Rose, Olivier Verscheure

For: STREAM CONTINUITY ENFORCEMENT

Enclosed are: [X] 21 sheets of specification; [X] 1 sheet(s) of Abstract; [X] 12 sheet(s) of claims; [X] 5 sheet(s) of drawing(s);

[X] An assignment of the invention to International Business Machines Corporation with Recordation Form.

[X] Declaration and Power of Attorney.

[ ] A certified copy of a ______________ application, from which priority under Title 35 USC §119 is claimed.

[X] Associate Power of Attorney.

The filing fee has been calculated as shown below:

	(Col. 1)	(Col. 2)	OTHER THAN A SMALL ENTITY	
FOR:	NO. FILED	NO. EXTRA	RATE	FEE
BASIC FEE				$ 690.00
TOTAL CLAIMS	34 -20 =	14	X $18 =	$ 252.00
INDEP CLAIMS	8 -3 =	5	X $78 =	$ 390.00
__ MULTIPLE DEPENDENT CLAIMS PRESENTED			+ 260 =	
			TOTAL	$ 1,332.00

If the difference in Col. 1 is less than zero, enter "0" in Col. 2.

[ ] Checks in the amount of $____ and $___ to cover the filing fee(s) and recording fee are enclosed.

[X] Please charge my Deposit Account No. 50-0510/IBM (Yorktown Heights) in the amount of $1,332.00

[X] The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 50-0510/IBM (Yorktown Heights). **A duplicate copy of this sheet is enclosed.**

[X] Any additional filing fees required under 37 CFR 1.16.

[X] Any patent application processing fees under 35 CFR 1.17.

Respectfully submitted,

By: James J. Bitetto

James J. Bitetto
Registration No. 40,513
Attorney for:
IBM Corporation
Intellectual Property Law Dept.
P.O. Box 218
Yorktown Heights, NY 10598

Please address all
correspondence to:
F. CHAU & ASSOCIATES, LLP
1900 Hempstead Turnpike, Suite 501
East Meadow, NY 11554
Tel: (516) 357-0091
Fax: (516) 357-0092

CERTIFICATION UNDER 37 C.F.R. § 1.10

I hereby certify that this Application transmittal and the documents referred to as enclosed are being deposited with the United States Postal Service on this date March 17, 2000 in an envelope as "Express Mail Post Office to Addressee" Mailing Label Number EL433927561US addressed to: Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231.

James J. Bitetto

James J. Bitetto

Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	YOR000028US1 (8728-349)
First Inventor or Application Identifier	Kienzle et al.
Title	Stream Continuity Enforcement
Express Mail Label No.	EL433927561US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ * Fee Transmittal Form *(e.g., PTO/SB/17)*
(Submit an original and a duplicate for fee processing)
2. ☒ Specification [*Total Pages* 34]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed)*
- Detailed Description
- Claim(s)
- Abstract of the Disclosure
3. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 5]
4. Oath or Declaration [*Total Pages* 2]
a. ☒ Newly executed (original or copy)
b. □ Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)
i. □ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

*** *NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).***

5. □ Microfiche Computer Program *(Appendix)*
6. Nucleotide and/or Amino Acid Sequence Submission
(*if applicable, all necessary)*
a. □ Computer Readable Copy
b. □ Paper Copy (identical to computer copy)
c. □ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s))
8. □ 37 C.F.R.§3.73(b) Statement *(when there is an assignee)* ☒ Power of Attorney
9. □ English Translation Document *(if applicable)*
10. ☒ Information Disclosure Statement (IDS)/PTO-1449 ☒ Copies of IDS Citations
11. □ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. □ * Small Entity Statement(s) *(PTO/SB/09-12)* □ Statement filed in prior application, Status still proper and desired
14. □ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. ☒ Other: Associate Power of Attorney

16. **If a CONTINUING APPLICATION,** *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No: ______/______
Prior application information: Examiner ______ *Group / Art Unit:* ______

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

□ *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* or □ *Correspondence address below*

Name	James J. Bitetto				
Address	F. Chau & Associates, LLP 1900 Hempstead Turnpike, Suite 501				
City	East Meadow	*State*	New York	*Zip Code*	11554
Country	USA	*Telephone*	(516) 357-0091	*Fax*	(516) 357-0092

Name (Print/Type)	James J. Bitetto	*Registration No. (Attorney/Agent)*	40,513
Signature	James J. Bitetto	*Date*	3/17/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

STREAM CONTINUITY ENFORCEMENT

BACKGROUND OF THE INVENTION

1. **Field of the Invention**

The present invention relates to digital multimedia stream distribution, and more particularly to a system and method to protect digital multimedia streams from unauthorized editing. The present invention may be employed for a plurality of different applications and may be particularly useful with regard to the commercial distribution of copyrighted works or other proprietary subject matter over either a public network or a physical storage medium, for example, DVD.

2. **Description of the Related Art**

With the advent of public computer networks, and the Internet, authors of digital media have an inexpensive means to distribute their works to a growing and massive audience. Consumers thus benefit from improved access to information and greater convenience. While artists and businesses benefit from distribution channels with enormous potential to reach a wide and varying client base.

Despite this potential, content providers have been reluctant to embrace this market. One hurdle to be overcome is a fundamental problem in the digital world, as opposed to the analog world. This fundamental problem is that an unlimited number of perfect editing operations can be made on any piece of digital content. A perfect edition means that no degradation is introduced by the editing operation. For example, one can easily get rid of some or all the commercials intentionally embedded in a movie. The resulting "commercial-free" movie can be distributed without quality difference from the unedited one.

The research area of "copyright protection" brings adequate solutions to this problem. Two typical technologies for copyright protection include "cryptography" and "steganography."

"Cryptography" is a field covering numerous techniques for scrambling information conveying messages so that when the message is conveyed between the sender and the receiver, a malicious party who intercepts this message cannot read it, edit it nor extract useful information from it. Once the content has been scrambled it cannot be used until it is unscrambled. Unscrambling requires the possession of a special key.

"Steganography" is a field covering numerous methods for hiding an informational message within some other medium in such a way that a malicious party who intercepts the medium carrying the hidden message does not know it contains this hidden message, for example a hidden watermark. Assuming the malicious party knows that the medium contains a hidden message, steganography makes it extremely difficult to extract it for further reading or editing.

Although these technologies provide protection from copying documents, a need exists to prevent the editing of documents by the addition or removal of portions of the document.

SUMMARY OF THE INVENTION

A system for enforcing data stream continuity, in accordance with the present invention, includes a server coupled to a transmission link for providing a data stream to at least one client over the transmission link. The data stream is segmented into units. The server includes a scrambler for encrypting at least one first unit using an encryption, and a steganographic unit for embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by the client to determine the encryption key and decipher the data stream.

In alternate embodiments, the steganographic unit preferably employs a steganographic masking algorithm. The data stream may include a transmission order which alternates between first units and second units. The steganographic unit preferably encrypts the at least one second unit. The at least one first unit and the at least one second unit may be encrypted and each may carry a portion of the encryption key. The transmission link may include the Internet. At least one of the client and the server may include a memory storage device.

Another system for enforcing data stream continuity includes a client system coupled to a transmission link for receiving a data stream from at least one server over the transmission link. The data stream is segmented into units. The client system includes a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server such that steganographic information is needed by the client to determine the encryption key. A descrambler descrambles at least one second unit which was encrypted in accordance with the encryption key before transmission from the server. A decoder is coupled to the key extractor and the descrambler for reassembling the data stream such that all of the units of the data stream are needed to decipher the data stream.

In alternate embodiments, the data stream may include a transmission order which alternates between first units and second units. The encryption key may also be steganographically hidden in the at least one second unit. The at least one first unit and the at least one second unit may be encrypted and each may carry a portion of the encryption key. The transmission link may include the Internet. At least one of the client and the server may include a memory storage device.

A method for enforcing data stream continuity, in accordance with the present invention, includes the steps of providing data to be transmitted over a link, segmenting the data into units for a data stream to be transferred over the link, scrambling at least one first unit by encrypting the at least one first unit using an encryption key, steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream, extracting the encryption key steganographically embedded in the at least one second unit in the data stream, descrambling at least one first unit which was encrypted in accordance with the encryption key and reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

Another method for enforcing data stream continuity, in accordance with the present invention includes providing data to be transmitted over a link, segmenting the data into units for a data stream to be transferred over the link, scrambling at least one first unit by encrypting the at least one first unit using an encryption key and steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream.

Yet, another method for enforcing data stream continuity, in accordance with the present invention, includes providing data segmented into units for a data stream transferred over the link, the units including at least one first unit and at least one second unit, extracting an encryption key steganographically embedded in the at least one second unit in the data stream, descrambling the at least one first unit which was encrypted in accordance with the encryption key and reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

In other methods, the data stream may include a transmission order which alternates between first units and second units. The step of steganographically embedding may include the step of steganographically embedding portions of the encryption key in the at least one first unit. The at least one first unit and the at least one second unit may be encrypted and may each carry a portion of the encryption key. The link may include the Internet. At least one of the client and the server may include a memory storage device. The methods and/or method steps may be implemented by a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform the method steps for enforcing data stream continuity in accordance with the invention.

These and other objects, features and advantages of the present invention will become apparent from the following detailed description of illustrative embodiments thereof, which is to be read in connection with the accompanying drawings.

BRIEF DESCRIPTION OF DRAWINGS

The invention will be described in detail in the following description of preferred embodiments with reference to the following figures wherein:

FIG. 1 is a block/flow diagram illustrating a system and method for protecting a music data stream from unauthorized editing in accordance with the present invention;

FIG. 2 depicts a digital multimedia stream which is decomposed into units including $\{C_i\}$ and $\{S_i\}$ in accordance with the present invention;

FIG. 3 depicts another embodiment of the present invention showing every unit from set $\{C_i\}$ including a portion of hidden key K_i that is used to encrypt/decrypt every unit from set $\{S_i\}$;

FIG. 4 depicts another embodiment of the present invention showing all units encrypted and hiding a portion of the encryption key; and

FIG. 5 is a block/flow diagram illustrating a system and method for protecting a digital data stream from unauthorized editing in accordance with the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention includes a system and method for protecting a digital multimedia stream against unauthorized editing. The present invention employs cryptographic and steganographic methods. By the present invention, a digital multimedia stream is divided up into units. The system and method enforce the continuity of two successive units i and i+1. The unit i includes an encryption key embedded using a steganographic function. The unit i+1 is encrypted using the key hidden in unit i. The system and method make it extremely difficult to edit the digital stream if the steganographic function is not possessed by the unauthorized person.

A digital multimedia distribution system of the present invention is useful in a variety of applications where it is desired to protect multimedia streams from unauthorized editing. Unauthorized editing includes, among many others, FBI warning message removal, advertising clips suppression, sound bytes removal, altering video segments or any other removal or addition of data to a data stream or stored media. The present invention has very broad applications and may be employed form any data stream or stored data. In one implementation, the present invention is employed to distribute digital music, video, text documents or any other data stream across a network or between a server and a client. The network may include a private network or a public network, such as, for example, the Internet. The server may include a VCR, a computer, a modem, a video player, a compact disc player, a wireless transmission device, a tape player or other transmission device or memory storage device. The client may include a VCR, a computer, a modem, a video player, a compact disc player, a wireless receiver device, a tape player or other receiver device or memory storage device.

It should be understood that the elements shown in FIGS. 1-4 may be implemented in various forms of hardware, software or combinations thereof. Preferably, these elements are implemented in software on one or more appropriately programmed general purpose digital computers having a processor and memory and input/output interfaces. Further, clients and servers (or client and server systems), as described herein, may apply to software applications, hardware devices or a combination thereof. Clients and servers may be resident on the same device or on a different devices.

Referring now to the drawings in which like numerals represent the same or similar elements and initially to FIG. 1, an illustrative system/method for employing one embodiment of the present invention is shown.

The present invention will now be described illustratively in terms of an example including a music data stream. The present invention should not be construed as limited by this example. FIG. 1 illustrates a digital music distribution system 10. The system 10 includes a data provider 200, such as, for example, a music provider, an advertiser 300 or alternate source of data, a server system 100, a network 500, such as a public network (e.g., the Internet) and a client 400. It is to be understood that multiple clients or servers may be employed in system 10. The music provider 200 and the advertiser 300 are shown to illustrate how multiple sources may include data into a data stream; however a single data source, such as a storage medium or a data source may be employed, as well as a plurality of data sources.

In the example, the music provider 200 and the advertiser 300 provide the music server system 100 with, for example, MP3-encoded music and short commercial audio clips, respectively. Upon request, the music server system 100 provides the client 400 with an editing-proof audio stream $\{C'_1, E_{K1}(S_1)\}$. The data stream, $\{C'_1, E_{K1}(S_1)\}$, is generated by segmenting the data stream into units.

Within the music server 100, an x-bit key generator 105 generates a key K_1. A steganographic function or algorithm 110 hides the randomly-generated key K_1 into a short commercial audio clip, C_1, provided by the advertiser 200. This generates C'_1. Then, a scrambler 115 encrypts an MP3-encoded music clip, S_1, provided by the music provider 300 using key K_1. This generates $E_{K1}(S_1)$. The music server system 100 distributes the digital stream $\{C'_1, E_{K1}(S_1)\}$ resulting from the concatenation of the short commercial audio clip including the key K_1,C'_1, and the scrambled digital music clip, $E_{K1}(S_1)$.

Upon reception of $\{C'_1,E_{K1}(S_1)\}$, the client system 400 first extracts the key K_1 from C'_1 using key extractor 405. The key is passed on to the descrambler 410, and is used to decrypt $E_{K1}(S_1)$. An MP3 decoder 415 sequentially decodes C_1 and S_1. C_1 and S_1 may be rendered by an audio renderer 420.

The client system 400 may function as a "blackbox." That is, the client may not have access to the digital audio streams C_1 nor S_1. The client has access to the analog audio coming out of the audio renderer 420.

The present invention can be applied to any digital content. The digital content is preferably capable of embedding temporal synchronization information. For example, the present invention may be applied to MPEG-4 multimedia streams including synchronized text, audio and video objects. Assume, for example, an MPEG-4 stream includes a text object to be displayed at time t_1, followed by an audio clip to be rendered at time t_2. The text and audio objects may correspond, respectively, to C_1 and S_1. In this case, the text object hides the key used to encrypt/decrypt the audio object.

The present invention assumes that both the steganographic function and the cryptographic algorithm used to, respectively, hide the key into a media unit and encrypt a following media unit, are not known by an unauthorized person. Cryptographic algorithms are often published, while stenographic systems have their mechanisms kept confidential and subject to non-disclosure agreements. Therefore, if the key cannot be extracted, guessing the cryptographic technique does not help in any way.

Cryptographic algorithms may include, for example, Rivest, Shamir and Adelmen (RSA), Data Encryption Algorithm (DEA) and the like. Steganographic techniques preferably provide a hidden key which does not affect the quality of the original signal, for example, the audio quality. Also, the hidden key should be statistically invisible. For example, an unauthorized person should not be able to detect the hidden key by comparing several signals belonging to the same content provider. The hidden key may be made such that it does not survive successive compression operations and/or signal manipulations.

A preferred steganographic technique for MP3-encoded audio exploits the masking properties of the human auditory system. Masking is a phenomenon in which one sound interferes with a persons perception of another sound. Frequency masking occurs when two tones which are close in frequency are played at the same time. Similarly, temporal masking occurs when a low-level signal is played immediately before or after a stronger one. Many stenographic techniques operate in this transform space. Stenographic techniques known in the art may be employed in accordance with the present invention.

Referring to FIG. 2, the present invention can also assist in preventing, for example, MPEG-2 movie broadcasts from commercial removal. A digital multimedia stream 600 is decomposed into units 602. Units 602 may include two sets of units, namely $\{C_i\}$ and $\{S_1\}$. A given unit C_j is immediately followed by unit S_j and preceded by unit S_{j-1}. In this case, $\{C_1\}$ and $\{S_i\}$ correspond respectively to the commercials and the movie clips in between commercials. The commercials represented by C_1, C_2,and C_3 in FIG. 2 are not encrypted and hide a set of keys $\{K_i\}$ used to encrypt/decrypt the movie clips S_1 and S_2. This information is processed the client system 400 as described with reference to FIG. 1.

Referring to FIG. 3, another implementation of the present invention is illustratively shown in accordance with the present invention. A digital multimedia stream 700 is decomposed into units 702. Every unit 702 from set $\{C_i\}$

includes a hidden key K_i that is used to encrypt/decrypt every unit from set $\{S_i\}$. Units C_i are not encrypted. This information is processed the client system 400 as described with reference to FIG. 1.

Referring to FIG. 4, another implementation of the present invention is illustratively shown in accordance with the present invention. A digital multimedia stream 800 is decomposed into units 802. All units 802 are encrypted and hiding a key. A first unit, C_0, is not encrypted.

Referring to FIG. 5, a digital data distribution system 900 is shown. The system 900 includes a data provider 902, such as, for example, a video provider, a music provider (FIG. 1), text, images or any other data which can be transmitted over a link. An alternate source of data 904 or redundant data from data provider 902 may be employed to alternately place units onto link 903. In this way, data provider represents C_i and alternate source of data 904 or redundant data represents S_i (see, e.g., FIG. 2).

The present invention may be applied on a single media (e.g., a movie or song) that has been broken up into units. The hidden key extraction algorithm should be capable of detecting a key without knowledge of the key's location in the media. Units may be of variable size (e.g., in bytes or in time (seconds)).

A server system 906 is coupled to a client 908 by link 903. Link 903 may include a network, such as a public network (e.g., the Internet) or a cable linking two devices, a wireless connection, a virtual circuit, a software link (or a link realized through a software application) or any other link in which data may be transferred. It is to be understood that multiple clients or servers may be employed in system 900.

The data provider 902 and the alternate data source 904 are shown to illustrate how multiple sources may include data into a data stream; however a single data source, such as a storage medium or a data source may be employed, as well as a plurality of data sources to place multiple data units in a predetermined order on link 903.

In the example, the data provider 902 and the alternate data source 902 provide the server system 906 with, for example, encoded (or encrypted) data units and key carrying data units (which may also be encrypted), respectively.

Upon request, the server system 906 provides a client 908 with an editing-proof data stream $\{C'_i, E_{Ki}(S_1)\}$, where K_i is an x-bit key, S_i is data from source 902, C'_i is a container for K_i and E_{Ki} is an encryption function using key K_i. The data stream, $\{C'_1, E_{K1}(S_1)\}$, is generated by segmenting the data stream into units.

An x-bit key generator 910 generates a key K_1. A steganographic algorithm 912 hides the randomly-generated key K_1 into data, C_1, provided by alternate data source 904. This generates C'_1. Then, a scrambler 914 encrypts, S_1, provided by the data source 902 using key K_1. This generates $E_{K1}(S_1)$. The server system 906 distributes the digital stream $\{C'_1, E_{K1}(S_1)\}$ resulting from the concatenation of the data from source 904 including the key K_1, C'_1, and the scrambled digital data from 902, $E_{K1}(S_1)$. This is performed by preferably employing a multiplexor 911.

Upon reception of $\{C'_1, E_{K1}(S_1)\}$, the client system 908 first extracts the key K_1 from C'_1 by employing a key extractor 915. The key is passed on to a descrambler 916, and is used to decrypt $E_{K1}(S_1)$. A decoder 918 sequentially decodes C_1 and S_1 using a demultiplexor 913 for example.

This reassembles the data stream to provide the original data package. C_1 and S_1 may be rendered by an renderer 920.

By the present invention, the encryption key K_1 is distributed across the transmission. Advantageously, to render the entire document transferred in the data stream, the entire document needs to be received. Any portion removed or added destroyed the encryption link between segments thereby ensuring unauthorized editing does not take place. The renderer 920 may include a video player, a tape player, a computer, a compact disc or DVD player, or any other storage media rendering device.

Having described preferred embodiments of a system and method for stream continuity enforcement (which are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. It is therefore to be understood that changes may be made in the particular embodiments of the invention disclosed which are within the scope and spirit of the invention as outlined by the appended claims. Having thus described the invention with the details and particularity required by the patent laws, what is claimed and desired protected by Letters Patent is set forth in the appended claims.

WHAT IS CLAIMED IS:

1. A system for enforcing data stream continuity comprising:

a server coupled to a transmission link for providing a data stream to at least one client over the transmission link, the data stream being segmented into units, the server including:

a scrambler for encrypting at least one first unit using an encryption key;

a steganographic unit for embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by the client to determine the encryption key and decipher the data stream.

2. The system as recited in claim 1, wherein the steganographic unit employs a steganographic masking algorithm.

3. The system as recited in claim 1, wherein the data stream includes a transmission order which alternates between first units and second units.

4. The system as recited in claim 1, wherein the steganographic unit encrypts the at least one second unit.

5. The system as recited in claim 1, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

6. The system as recited in claim 1, wherein the transmission link includes the Internet.

7. The system as recited in claim 1, wherein at least one of the client and the server include a memory storage device.

8. A system for enforcing data stream continuity comprising:

a client system coupled to a transmission link for receiving a data stream from at least one server over the transmission link, the data stream being segmented into units, the client system including:

a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server such that steganographic information is needed by the client to determine the encryption key;

a descrambler for descrambling at least one second unit which was encrypted in accordance with the encryption key before transmission from the server; and

a decoder coupled to the key extractor and the descrambler for reassembling the data stream such that all of the units of the data stream are needed to decipher the data stream.

9. The system as recited in claim 8, wherein the data stream includes a transmission order which alternates between first units and second units.

10. The system as recited in claim 8, wherein the encryption key is also steganographically hidden in the at least one second unit.

11. The system as recited in claim 8, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

12. The system as recited in claim 8, wherein the transmission link includes the Internet.

13. The system as recited in claim 8, wherein at least one of the client and the server include a memory storage device.

14. A method for enforcing data stream continuity comprising the steps of:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key;

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream;

extracting the encryption key steganographically embedded in the at least one second unit in the data stream;

descrambling at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

15. The method as recited in claim 14, wherein the data stream includes a transmission order which alternates between first units and second units.

16. The method as recited in claim 14, wherein the step of steganographically embedding includes the step of steganographically embedding portions of the encryption key in the at least one first unit.

17. The method as recited in claim 14, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

18. The method as recited in claim 14, wherein the link includes the Internet.

19. The method as recited in claim 14, wherein at least one of the client and the server include a memory storage device.

20. A method for enforcing data stream continuity comprising the steps of:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key; and

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream.

21. The method as recited in claim 20, wherein the data stream includes a transmission order which alternates between first units and second units.

22. The method as recited in claim 20, wherein the step of steganographically embedding includes the step of steganographically embedding portions of the encryption key in the at least one first unit.

23. The method as recited in claim 20, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

24. The method as recited in claim 20, wherein the link includes the Internet.

25. The method as recited in claim 20, wherein at least one of the client and the server include a memory storage device.

26. A method for enforcing data stream continuity comprising the steps of:

providing data segmented into units for a data stream transferred over the link, the units including at least one first unit and at least one second unit;

extracting an encryption key steganographically embedded in the at least one second unit in the data stream;

descrambling the at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

27. The method as recited in claim 26, wherein the data stream includes a transmission order which alternates between first units and second units.

28. The method as recited in claim 26, wherein the portions of the encryption key are embedded in the at least one first unit.

29. The method as recited in claim 26, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

30. The method as recited in claim 26 wherein the link includes the Internet.

31. The method as recited in claim 14, wherein at least one of the client and the server include a memory storage device.

32. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enforcing data stream continuity, the method steps comprising:

segmenting data to be transmitted over a link into units for a data stream to be transferred over the link;

scrambling at least one first unit for the data stream before transmission by encrypting the at least one first unit using an encryption key; and

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream;

extracting the encryption key steganographically embedded in the at least one second unit in the data stream;

descrambling at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

33. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enforcing data stream continuity, the method steps comprising:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key; and

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream.

34. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enforcing data stream continuity, the method steps comprising:

providing data segmented into units for a data stream transferred over the link, the units including at least one first unit and at least one second unit;

extracting an encryption key steganographically embedded in the at least one second unit in the data stream;

descrambling the at least one first unit which was encrypted in accordance with the encryption key; and reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

STREAM CONTINUITY ENFORCEMENT

ABSTRACT OF THE DISCLOSURE

A system for enforcing data stream continuity, in accordance with the present invention, includes a server coupled to a transmission link for providing a data stream to at least one client over the transmission link. The data stream is segmented into units. The server includes a scrambler for encrypting at least one first unit using an encryption key, and a steganographic unit for embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by the client to determine the encryption key and decipher the data stream.

1/5
Kienzle et al.
YOR000028US1 (DMS) (8728-349)

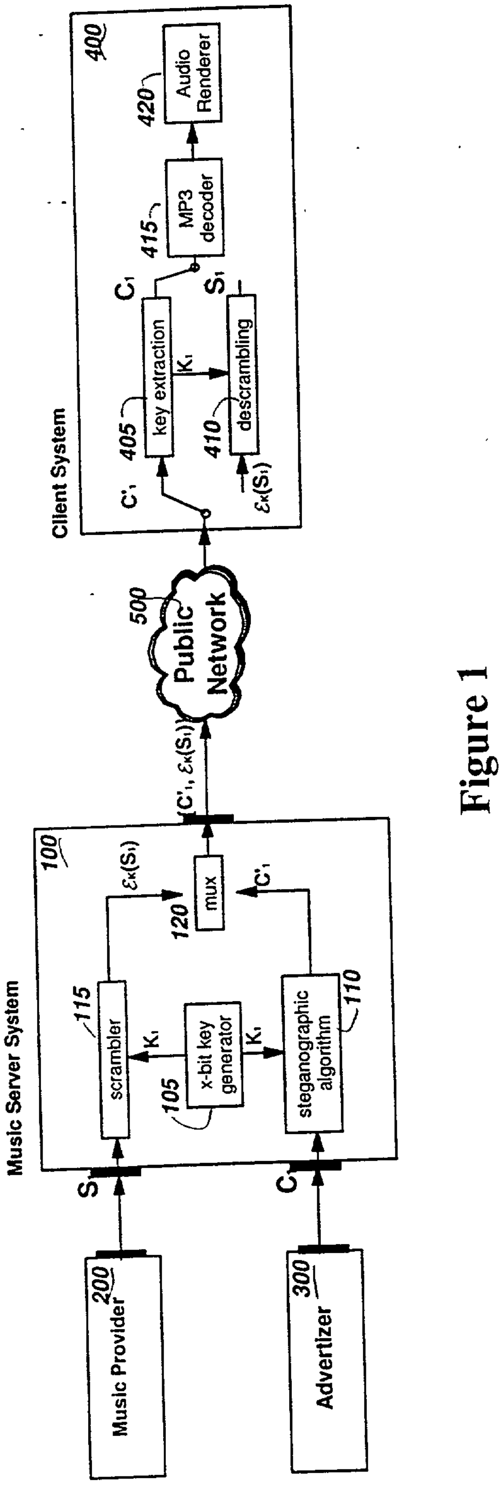

Figure 1

12

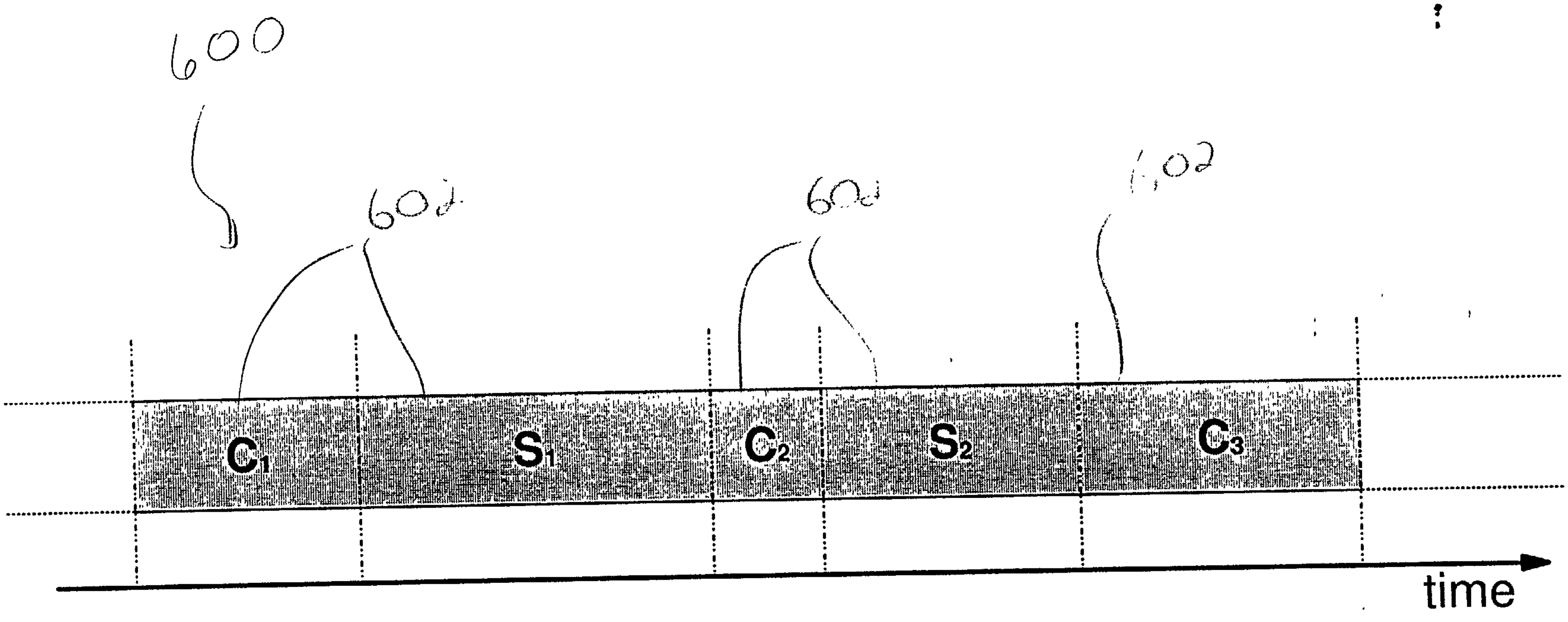

Figure 2

2/5
YOR000028US1 (8728-349)

3/5
YOR000028US1 (8728-349)

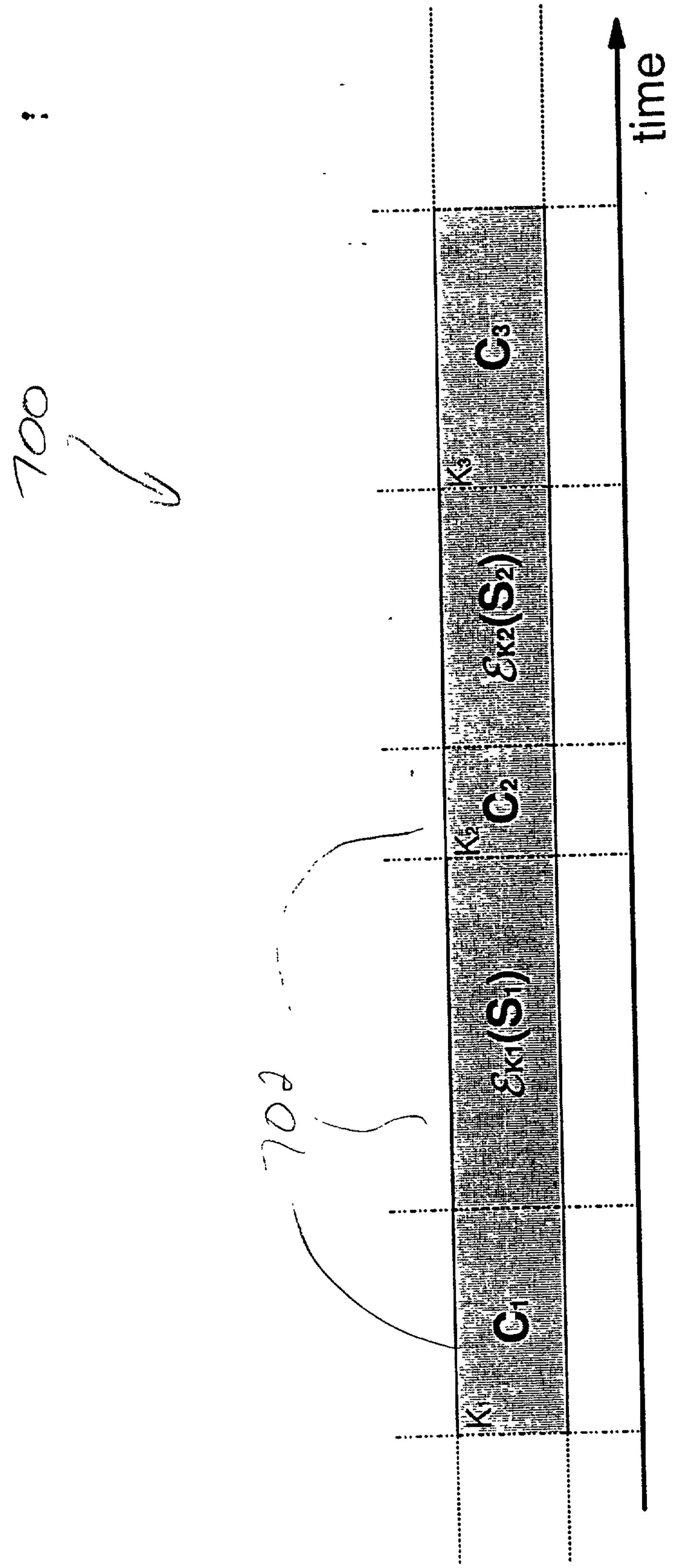

Figure 3

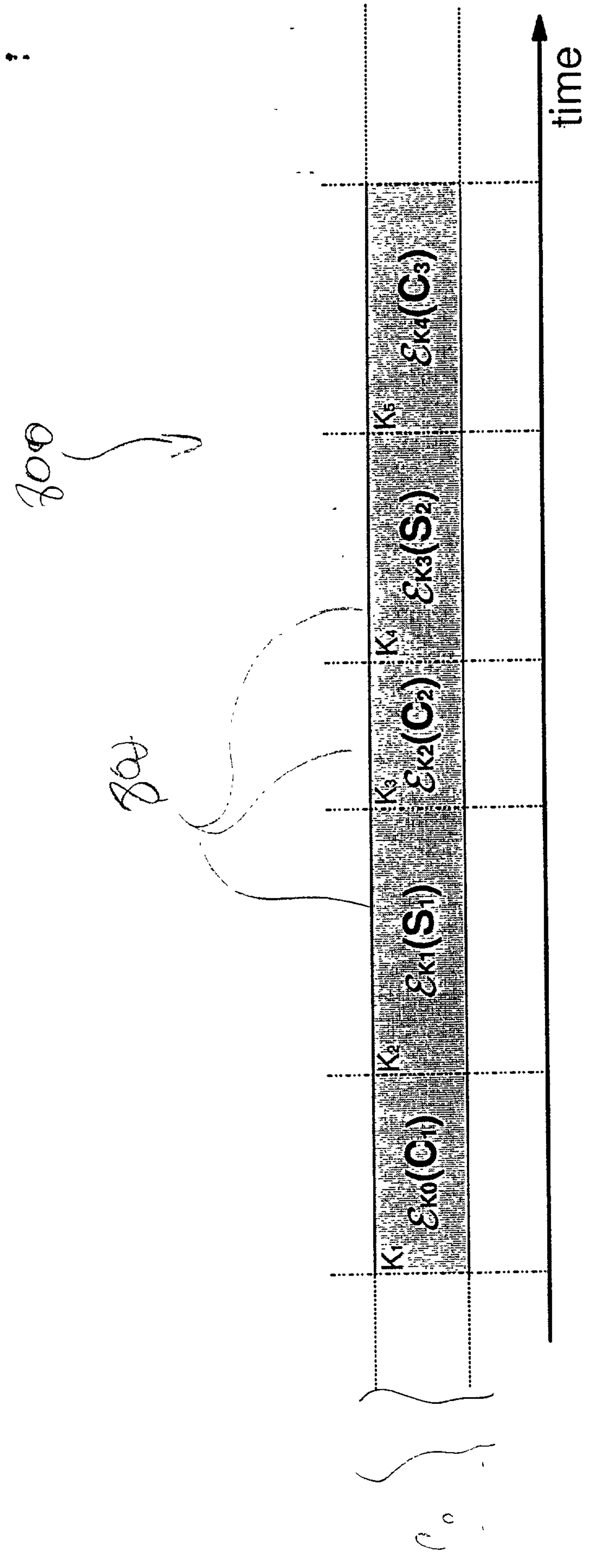
time
K1
$\mathcal{E}_{K0}(C_1)$
K2
$\mathcal{E}_{K1}(S_1)$
K3
$\mathcal{E}_{K2}(C_2)$
K4
$\mathcal{E}_{K3}(S_2)$
K5
$\mathcal{E}_{K4}(C_3)$
300
302

Figure 4

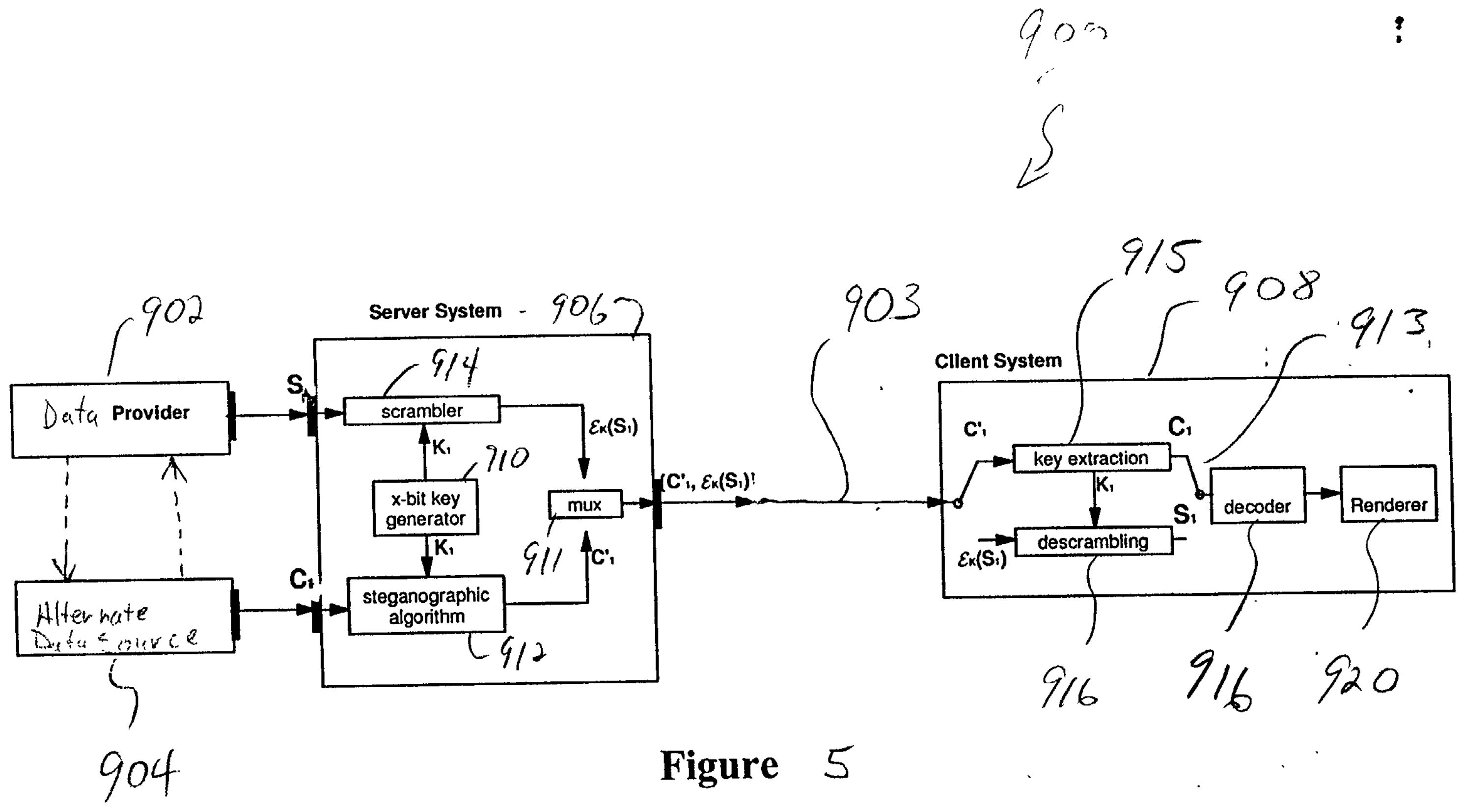
900
902
Data Provider
Alternate Data Source
904
S1
C1
Server System - 906
914
scrambler
K1
910
x-bit key generator
K1
steganographic algorithm
912
εK(S1)
mux
911
C'1
(C'1, εK(S1))
903
Client System
915
908
913
C'1
key extraction
C1
K1
S1
εK(S1)
descrambling
decoder
Renderer
916
916
920

Figure 5

DECLARATION Attorney Docket No. YOR000028US1 (8728-349)

AS A BELOW NAMED INVENTOR, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe that I am the original, first and sole *(if only one name is listed below)*, or an original, first and joint inventor *(if plural names are listed below)*, of the subject matter which is claimed and for which a patent is sought on the invention entitled:

TITLE: **STREAM CONTINUITY ENFORCEMENT**

the specification of which either is attached hereto or indicates an attorney docket no. YOR000028US1 (8728-349), or:

□ was filed in the U.S. Patent & Trademark Office on ________ and assigned Serial No. ______,

□ and *(if applicable)* was amended on ____,

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability and to the examination of this application in accordance with Title 37 of the Code of Federal Regulations §1.56. I hereby claim foreign priority benefits under Title 35, U.S. Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States, listed below and have also identified below any foreign applications for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

			Priority Claimed:
(Application Number)	*(Country)*	*(Day/Month/Year filed)*	Yes [ ] No [ ]
(Application Number)	*(Country)*	*(Day/Month/Year filed)*	Yes [ ] No [ ]

I hereby claim the benefit under Title 35, U.S. Code, §120 of any United States application(s), or §119(e) of any United States provisional application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application(s) in the manner provided by the first paragraph of Title 35, U.S. Code, §112, I acknowledge the duty to disclose information material to patentability as defined in Title 37, The Code of Federal Regulations, §1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial Number)	*(Filing Date)*	*(STATUS: patented, pending, abandoned)*
(Application Serial Number)	*(Filing Date)*	*(STATUS: patented, pending, abandoned)*

I hereby appoint the following attorneys: **MANNY W. SCHECTER**, Reg. No. 31,722; **TERRY J. ILARDI**, Reg. 29,936; **CHRISTOPHER A. HUGHES**, Reg. No. 26,914; **EDWARD A. PENNINGTON**, Reg. No. 32,588; **JOHN E. HOEL**, Reg. No. 26,279; **JOSEPH C. REDMOND, Jr.**, Reg. No. 18,753; **WAYNE L. ELLENBOGEN**, Reg. No. 43,602; **STEPHEN C. KAUFMAN**, Reg. No. 29,551; **JAY P. SBROLLINI**, Reg. No. 36,266; **DAVID M. SHOFI**, Reg. No. 39,835; **ROBERT M. TREPP**, Reg. No. 25,933; **LOUIS P. HERZBERG**, Reg. No. 41,500; **DANIEL P. MORRIS**, Reg. No. 32,053; **DOUGLAS W. CAMERON**, Reg. No. 31,596; **LOUIS J. PERCELLO**, Reg. No. 33,206; and **PAUL J. OTTERSTEDT**, Reg. No. 37,411; each of them of **INTERNATIONAL BUSINESS MACHINES CORPORATION**, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598; to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith and with any divisional, continuation, continuation-in-part, reissue or re-examination application, with full power of appointment and with full power to substitute an associate attorney or agent, and to receive all patents which may issue thereon, and request that all correspondence be addressed to:

Frank Chau, Esq.
F. CHAU & ASSOCIATES, LLP
1900 Hempstead Turnpike, Suite 501
East Meadow, New York 11554
Tel.: 516-357-0091

I HEREBY DECLARE that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 U.S. Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF FIRST OR SOLE INVENTOR: Martin Kienzle Citizenship German

Inventor's signature: Martin Kienzle Date: 3/14/2000

Residence & Post Office Address: 19 Woodfield Road
Briarcliff Manor, NY 10510

FULL NAME OF SECOND JOINT INVENTOR: Ray E. Rose Citizenship U.S.A.

Inventor's signature: Raymond E Rose Date: 3/14/2000

Residence & Post Office Address: David Drive
Purdys, NY 10578

FULL NAME OF THIRD JOINT INVENTOR: Olivier Verscheure Citizenship Belgian

Inventor's signature: Date: 03/14/00

Residence & Post Office Address: 30-61 47th Street
Long Island City, NY 11103

FULL NAME OF FOURTH JOINT INVENTOR: Citizenship

Inventor's signature: Date:

Residence & Post Office Address:

FULL NAME OF FIFTH JOINT INVENTOR: Citizenship

Inventor's signature: Date:

Residence & Post Office Address:

FULL NAME OF SIXTH JOINT INVENTOR: Citizenship

Inventor's signature: Date:

Residence & Post Office Address:

Attorney Docket No. YOR000028US1 (8728-349)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S): Martin Kienzle, Ray E. Rose, Olivier Verscheure

SERIAL NO.: Unassigned

FILED: Concurrently herewith

FOR: STREAM CONTINUITY ENFORCEMENT

ASSOCIATE POWER OF ATTORNEY

Please recognize **FRANK CHAU**, Reg. No. 34,136; **JAMES J. BITETTO**, Reg. No. 40,513; **FRANK V. DeROSA**, Reg. No. 43,584; and **GASPARE J. RANDAZZO**, Reg. No. 41,528; each of them of **F. CHAU & ASSOCIATES, LLP**, 1900 Hempstead Turnpike, Suite 501, East Meadow, New York 11554 as associate attorneys in the above-mentioned application, with full power to prosecute said application, to make alterations and amendments therein, and to transact all business in the Patent and Trademark Office connected therewith.

Telephone calls should be made to Frank Chau by dialing (516) 357-0091.

All written communications are to be sent to Frank Chau, Esq., F. Chau & Associates, LLP, 1900 Hempstead Turnpike, Suite 501, East Meadow, New York 11554.

International Business Machines
Corporation
T.J. Watson Research Center
Route 134 and Kitchawan Road
Yorktown Heights, New York 10598

Manny W. Schecter
Registration No. 31,722
David M. Shofi
Registration No. 39,835
Attorney for Applicant(s)